DoD's CIO and SECDEF Special Assistant for C3I Matters, Speaks Out

Arthur L. Money Set to Help Lead DoD Into Y2K and Beyond

Technology is growing at an alarming rate. What is cutting edge today is often outdated tomorrow. The key to survival in this "cyber age" is the ability to adapt one's computer and information systems to ride the changing waves of technology instead of being swallowed up by them.

The man responsible for not only safeguarding, but improving DoD's information systems into the next millennium is the "new" Special Assistant to the Secretary of Defense for Command, Control, Communications, and Intelligence (C3I) Matters and DoD Chief Information Officer, Arthur L. "Art" Money.

The versatile Money took over his current position Feb. 20, 1998, and until very recently, continued to serve as the Assistant Secretary of the Air Force for Acquisition, a position he had held since January 1996.

With more than 33 years' experience, Money brings with him an impressive résumé as he works with other DoD leaders to improve the "flow of information" across the Services and revolutionize the way DoD does business with regard to acquisition. In this interview, *Program Manager* attempts to relay the challenges facing Money as DoD braces for Y2K and beyond.

Q

As the Air Force's former Chief Information Officer [CIO] and Assistant Secretary of the Air Force for Acquisition, how has your perspective changed now that you have been on the job for a little over a year?

DSMC's Air Force Chair Tony Kausal (right) interviews Money in his Pentagon office.

A

Since leaving the Air Force and joining OSD [Office of the Secretary of Defense], I have learned that the need for jointness and interoperability across the Department is even more important than I initially believed. The flow of information does not stop at organizational boundaries. Consequently, as DoD CIO I am working toward bringing everyone together to adopt common architectures, standards, and frameworks across all of DoD and ensuring an uninterrupted flow of information end-to-end.

Q

Several Defense Reform Initiatives that received a fair amount of press dealt with extensive restructuring recommendations for the DoD's C3I office, including new missions. In response to that, in mid-1998 you

A special thanks to DSMC professor, George Prosnik and DSMC Air Force Chair, Tony Kausal for their contributions to this article.

Photos by Greg Caruth

spearheaded just such a reorganization effort. Could you summarize the resultant key organizational changes for our readers? How is the new organization working?

A

Indeed the Defense Reform Initiatives resulted in a great deal of change within C3I. Several of the existing C3I functions such as Year 2000, information protection and assurance, spectrum allocation, and electronic commerce were expanded, while at the same time, C3I received several new missions including critical infrastructure protection, space policy, and airborne reconnaissance oversight. A few of the major results of the changes in mission and the ensuing reorganization include greater attention and focus on the Year 2000 issue and the CIO function as a whole throughout the entire Department; the coupling of information assurance and critical infrastructure protection; and the alignment of all aspects of several functional areas (ISR [Intelligence, Surveillance, and Reconnaisance]; security; CIO; space and information). The restructuring of the organization and the development of our 10 goals have C3I as an organization moving in the right direction to lead the Department toward achieving Information Superiority.

"Since leaving the Air Force and joining OSD, I have learned that the need for jointness and interoperability across the Department is even more important than I initially believed. The flow of information does not stop at organizational boundaries."

Q

What are your top Departmental priorities beyond Y2K?

A

DoD has grown its networks from the ground up due to the strong institutional structure in place to support the 50-year-old military messaging system. Over the past five years we have seen an enormous growth in Commercial Off-the-Shelf [COTS]–based networks and computing capacity to the point that most primary functions ride this emerging infrastructure. Beyond Y2K, my highest priority is to put sufficient discipline into this global infrastructure to achieve Information Superiority and to provide a fully secure, reliable, interoperable computing and communications enabling capacity for everyone in DoD.

To aid in focusing our efforts to achieve information superiority, we have identified 10 goals within C3I. The first, of course, is ensure continuity of mission-essential DoD operations despite Y2K disruptions, and the remaining nine are:

- Implement effective programs for information assurance and critical infrastructure protection.
- Build a coherent global network based on efficient and effective DoD information architectures and procedures.
- Plan and implement a joint and combined end-to-end C3ISR and space integration.
- Establish a knowledge-based workforce within DoD.
- Establish policies and budget priorities that will lead to the reinvention of intelligence for the 21st century.
- Revise policies for information operations, security, and counterintelligence.
- Establish electronic commerce and business process change throughout the functional areas of DoD.
- Develop an advance technology plan for information superiority.
- Transform OASD(C3I) into a nurturing, caring organization that serves as a model team in attaining its goals.

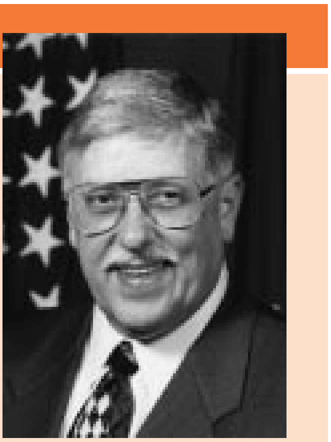
Q

Over the next three to five years, what do you view as the hottest IT [Information Technology] impacting DoD? How is your office "geared up" to assess and handle the increasing pace of technological change?

A

Though the Department will be impacted by technological change, our focus is not so much on hot new technologies, but rather on the emerging operational requirements of the warfighter. There is no doubt, though, that we see

Arthur L. Money



Special Assistant to the Secretary of Defense for C3I Matters and DoD Chief Information Officer

Arthur L. Money was appointed the Senior Civilian Official, Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) and Chief Information Officer of the Department of Defense February 20, 1998. May 24, 1999, his official title changed to Special Assistant to the Secretary of Defense for Command, Control, Communications, and Intelligence (C3I) Matters.

Money served as Assistant Secretary of the Air Force for Acquisition from January to May 1999.

He was President of ESL Inc., a subsidiary of TRW, before it was consolidated with TRW's Avionics and Surveillance Group, and Vice President and Deputy General Manager for the TRW Avionics and Surveillance Group. The group is internationally recognized for airborne electronic systems and technologies, including reconnaissance and intelligence systems and advanced integrated avionics.

Money has more than 33 years of management and engineering experience with the defense electronics and intelligence industry in the design and development of intelligence collection analysis capabilities and airborne tactical reconnaissance systems.

He is a graduate of San Jose State University, with a bachelor's degree in mechanical engineering. He received his master's degree in mechanical and electrical engineering from Santa Clara University.

As the Special Assistant to the Secretary of Defense for C3I Matters, Money is the principal staff assistant for Information Superiority. He provides overall policy and program guidance for DoD command, control, communications, computer, intelligence, surveillance, and reconnaissance activities; space and space systems; and information technology investments.

IT as a means to enhance the operational capabilities of DoD.

GNIE

For example, the Department has a major initiative underway to build a coherent Global Networked Information Enterprise [GNIE] based on efficient and effective DoD information architectures and procedures. The GNIE will provide the "information fabric" that brings the notion of a DoD enterprise and information superiority into reality, enabling the operational concepts of JV2010 [*Joint Vision 2010*]. GNIE policies, plans, and programs will embody the constructs that will create the computing model shift to information-centric operations/warfare. GNIE provides the means to structure the future of the Department's computing resources to achieve the reality of information superiority.

At the core of GNIE is the recognition of the pervasiveness and durability of distributed computing across DoD. Networked client/server (mid-tier) and Web-enabled architecture will define the core of the GNIE with the tenets of enterprise management, economies of scale, and information assurance governing its evolution. Thus the technologies in the following areas will play a large part in the success of the GNIE:

Client/Server and Distributed Computing. Though the technology may be considered "old hat stuff," it is clear that the new Web-enabled technologies are heavily dependent upon progress in the areas of distributed computing.

Information Assurance/Public Key Infrastructure (PKI). Public-key cryptography is fast becoming the foundation for online commerce and other applications that require security and authentication in an open network. The widespread use of public-key cryptography requires a public-key infrastructure to publish and manage public-key values. Without a functioning infrastructure, public-key cryptography is only marginally more useful than traditional, secret-key cryptography. Beyond PKI, the Department will pursue those technologies that provide a "Defense in depth" approach for mitigating risk.

Web-enabled Services. Services that allow the user to better locate and extract information "at any time, anywhere."

Quality of Service (QoS). The Department would prefer to avoid the solution of simply "overengineering the network" to achieve quick, consistent, and reliable information transfer –we would prefer to implement QoS systems features that give us cost-effective means of managing loss characteristics, avoiding and managing network congestion, shaping network traffic, and setting traffic priorities across the network. Though our strategies that take full advantage of COTS have provided great new opportunities, these strategies may not fill all the needs of the Department.

Current efforts have enabled the foundation for today's high-speed, secure information enterprise. Future information enterprise requirements will not be attainable unless we focus our research and development efforts. DoD must ensure that the sustaining R&D [Research & Development] base for the future information enterprise is a DDR&E/DARPA [Director, Defense Research & Engineering/Director, Advanced Research Projects Agency] priority – including enterprise control, intrusion detection, object-oriented databases, and other critical information technology areas.

One of the GNIE thrust areas will assist the Department in understanding the means to do so. One of the core products of this thrust area includes a report on critical technologies. The report will be available in the July 1999 timeframe.

Through the initiatives just discussed, we are striving to establish a foundation for the Joint Technical Architecture [JTA], DII Common Operating Environment [DII COE], system architectures, operational architectures, and ISR interoperability that will help enable the development of a knowledge-based workforce.

Q

Safeguarding the national infrastructure from cyber attack has become a recent high-visibility national priority. Your office plays a rather unique role dealing in this area, in coordinating DoD's efforts with activities such as the Commerce Department's Critical Infrastructure Assurance Office and the FBI's National Infrastructure Protection Center. Can you comment on how this relationship is working so far? What is the role of the recently formed Joint Task Force for Computer Network Defense?

A

Exercises like Eligible Receiver and real-world events like Solar Sunrise have helped DoD recognize the necessity for a coordinated approach to defending its computer networks. One of the biggest questions left unanswered was "Who's in charge?" The Joint Task Force for Computer Network Defense [JTF-CND] was created to help answer that question and to ensure that DoD works and coordinates together as a unit, and not only as individual Services and agencies. The JTF-CND is the first DoD-wide organization that serves as the focal point for defense of computer networks and systems. It takes advantage of the existing intrusion detection capabilities of its four military service components, the DoD Computer Emergency Response Team, and the unified commands and agencies. The JTF receives intrusion data from these DoD sources and then fuses this critical information along with ongoing operational missions, intelligence, and technical data into a "big picture" synopsis of the incident. The JTF works at the global (strategic) level and is the Department's primary interface with the FBI's National Infrastructure Protection Center.

With respect to critical infrastructure protection, we have created within DoD a Critical Infrastructure Protection Office [CIPO] to interface and work very closely with the national-level Critical Infrastructure Assurance Office [CIAO]. For example, CIPO has been a key player in the development of the National Plan. We have provided DoD assets to help staff the office, e.g., we have a defense liaison person on the CIAO staff and a person to work on the Expert Review Team. Although these organizations and relationships are only in the infancy stage, we feel like we're headed in the right direction and have positive and productive activities ongoing.

> "I am working toward bringing everyone together to adopt common architectures, standards, and frameworks across all of DoD, and an uninterrupted flow of information end-to-end."

Q

Because of their obvious potential payoffs, COTS products are being emphasized for DoD software-intensive systems. But use of such products can have a downside, notably in integration, quality, and support risks. Additionally, COTS products, being readily available, can be exhaustively analyzed by a potential adversary and thus may increase susceptibility of systems to so-called cyber attacks. Do you have any guidance as to how acquisition offices can achieve some balance in this area?

A

Exploiting COTS computer software products is one of the first software engineering principles listed in the DoD Acquisition Policy, 5000.2-R, and we do promote it in the oversight of major Automated Information Systems [AIS] acquisitions. It also gives us state-of-the-art capabilities quickly and allows us to move toward commercial best practices more easily than through the development of our own applications. Additionally, interoperability of business processes, e.g., Electronic Business/Electronic Commerce, is aided by the use of COTS products.

However, many programs encounter major problems when they try to modify their COTS products. Before starting a COTS software acquisition, program managers should do sufficient market research to determine whether a COTS package is available that can meet documented system requirements without modification. COTS software can be surrounded with functional layers that modify its inputs and outputs, but COTS software should rarely be modified.

Support, integration, and information assurance are also COTS issues that we are grappling with. There is guidance in the *Defense Acquisition Deskbook* and in various DoD-sponsored Web sites on these topics, and my office recently committed to the Department of Defense Inspector General to develop guidance in the next six to 12 months on the appropriate use of COTS software in major AIS acquisitions. At a minimum, that guidance will address such issues as modification of COTS software, rights to modify and maintain the software and related documentation, ownership of source code, and other lessons learned from ongoing acquisitions of COTS for major AIS.

Regarding information assurance, we are engaged in several initiatives that address overall security concerns, including those associated with COTS software. The Vulnerability Assessment Program provides expert analysis and testing of systems and provides program managers detailed citations of areas of actual penetration by professionals, and identifies solutions to close that penetration path. The Department has also initiated the Defense Information Assurance Program, which can aid the program manager to help understand security methods in the dynamic global information environment. This program provides a common specification language, evaluation methodology, and understanding of results for information assurance issues.

We have also found that many of our weaknesses/vulnerabilities are more likely to be as a result of inconsistent and incorrect product implementation and operation rather than inherent product vulnerabilities. Also, generally speaking, COTS products enjoy a widespread and active user base that is quick to identify and report deficiencies, faults, or vulnerabilities to the vendor. Many vendors are quick to react to discovered vulnerabilities and provide rapid patches/fixes to the user base.

Currently, we have IT policy undergoing review with change in several areas in mind. Certainly addressing the COTS issue is but one of these. It is paramount that we provide guidance for all to follow in this shared risk world so that we may be able to adequately protect our DoD enterprise from vulnerabilities.

Q

In one of DoD's streamlining initiatives, the venerable MAISRC [Major Automated Information Systems Review Council] was disestablished in July 1998 and replaced by the Information Technology OIPT [IT-OIPT]. How has this new IPT-based process been working?

A

This question gives me an opportunity to address an apparent misperception about the demise of the MAISRC. Too many people apparently believe that disestablishing the MAISRC signaled a lessening in oversight of major AIS by the DoD CIO. That is not the case. The rules that applied previous to MAISRC elimination (i.e., DoD Directive 5000.1 and DoD 5000.2-R) continue to apply. My office continues to oversee the major systems almost exactly as we did in the past. I continue to be the Milestone Decision Authority for major AIS, and we have held as many IPT meetings and issued as many, if not more, Acquisition Decision Memoranda as we did before the MAISRC was disestablished.

The "new IPT-based process" is working well because it is the same process we have followed since 1995 when the Secretary of Defense directed that all acquisition and oversight activities be conducted through the IPT process. At that time, my office and the Office of the USD(A&T) collaborated on a guidance document called "Rules of the Road: A Guide to Conducting IPT Meetings," which the Department has been following since that time. The IT OIPT was essentially a name change from the previous MAISRC OIPT that had existed for a number of years. When the IT OIPT cannot resolve an issue, my Deputy CIO or I hold a CIO review to resolve the issue.

Having said that, we are in the process of changing the focus of our oversight process to better implement the Clinger-Cohen Act and related IT reform legislation. We are building on the success of the Y2K effort by replacing system-focused oversight with a process that will require each IT investment to be placed into a mission or functional thread or "portfolio."

Under this new process, the DoD Deputy CIO will evaluate IT investments based on their value to the mission or functional thread of which they are a part. This should allow us to delegate more acquisition authority for individual systems to Component CIOs.

Q

In response to the National Research Council's Fall 1996 report on Ada, DoD is taking a "hands-off" position on mandating use of specific programming languages, including Ada. However, by some estimates, some 50 million lines of Ada code, primarily in weapons and C3I systems, still remain in the DoD inventory and need to be supported. What plans exist for sustaining this critical legacy code?

A

On April 29, 1997, the Department issued policy that requires programming language selections to be made "... in the context of the system and software engineering factors that influence overall life cycle costs, risks, and potential for interoperability." The guidance explicitly states that Ada should be one of the languages considered in this decision process, but does not require that Ada be selected. Thus, DoD policy now places all programming languages on equal footing, where capability to provide the best support to the mission requirement will drive the solution selected, not a "one size fits all" mandate.

Ada is a proven software language for warfighting and battlefield management applications. It is excellent for safety-critical systems. DoD is confident that an engineering approach to the programming language selection process will result in continued use of Ada for those applications that require its unique strengths.

Past DoD investments in this technology have facilitated Ada development, standardization, and the creation of a self-sustaining infrastructure. Today, the Ada Resource Association, a consortium of Ada compiler and tool vendors, has assumed many of the functions performed in the past by DoD's Ada Joint Program. Therefore, Ada development and support tools and resources should continue to be available.

Thus, DoD believes that Ada as a technology is here to stay. But like almost every other technology, it must evolve, and its long-term viability will be ultimately determined by the marketplace. In that context, future DoD decisions on building/maintaining/modernizing any code will continue to be made considering the marketplace, life cycle costs, system requirements, and other factors.

Q

Press reports continue to note persistent shortages of IT workers in the commercial sector. DoD has a particularly difficult problem in today's economy of retaining skilled high-technology workers. What are DoD's plans or initiatives to address long-term retention of DoD employees with critical technical skills?

A

The Department is pursuing a number of initiatives to acquire and retain technical personnel to effectively and efficiently carry out its diverse technology-based missions.

A DoD IPT was recently convened to examine issues pertaining to the training and retention of DoD Information Technology Management [ITM] personnel. The IPT's findings indicate the Department must create certain career management mechanisms to satisfy its training and retention goals.

Some of the team's recommended retention initiatives include:

- Establishing a central database of DoD ITM personnel.
- Identifying and maintaining a core ITM workforce capability within the Department.
- Creating a specialty skill tracking system with pay incentives, while allowing further professional development and career opportunities.

Other initiatives that are being reviewed for further study include:

- Establishing programs to acquire technical personnel with agreements to pay for civilian advanced education and technical training, with retention stipulations that would require the employee to stay within the Department of Defense for a set number of years.
- Establishing fellowship/cooperative programs with leading high-tech industry organizations.
- Creating special pay categories for hard-to-fill IT positions.

An adequately trained and experienced ITM workforce is a critical component in carrying out the Department's daily operational and warfighting missions. Therefore, the Department will do whatever it takes to retain its ITM personnel. Some of the DoD Components currently are recruiting at local colleges and universities, using special pay incentives, and offering educational opportunities to attract and retain IT technical expertise.

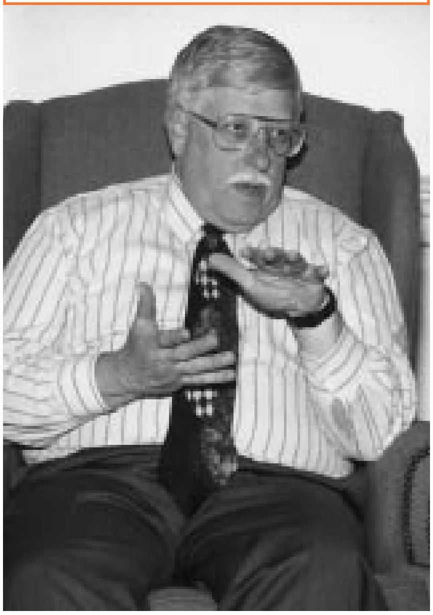
Q

In April 1998, Secretary Cohen, as part of his so called "912 Report to Congress," noted that, in order to address interoperability issues, you and the Under Secretary of Defense (Acquisition & Technology) would "examine ways to establish a joint command, control, and communications integrated system development process to guide design and achieve integrated systems development." What is the status of this effort? What changes can our readers expect to see in procurement and acquisition processes?

A

Section 912 of the FY 1998 Defense Authorization Act included several requirements related to acquisition. As you cited, Secretary Cohen's report to Congress covered some of these requirements. Specifically, the Secretary noted that "joint operations have been hindered by the inability of forces to share critical information at the rate and at the locations demanded by modern warfare." To address this problem, a Joint Command and Control Acquisition Study Group [JC2ASG] was established by the Under Secretary of Defense (Acquisition & Technology) [USD(A&T)] and me, composed of the commanders of the Services' Command and Control [C2] systems development/acquisition centers.

"Though the Department will be impacted by technological change, our focus is not so much on hot new technologies, but rather on the emerging operational requirements of the warfighter. There is no doubt, though, that we see IT as a means to enhance the operational capabilities of DoD."



The three commands are the Army's Communications-Electronics Command [CECOM], the Air Force's Electronic Systems Center [ESC], and the Navy's Space and Naval Warfare Systems Command [SPAWAR]. These commands, together with inputs from the staffs of USD(A&T), ASD(C3I), DISA, Joint Staff, and Service C4I Chiefs, examined processes, management structures, and forums to implement joint C2 Integration/Interoperability [I2] among the Services to ensure that:

- Future efforts will be "Joint First."
- Joint C2I2 will be advanced at every opportunity.
- I2 opportunities discovered through joint experimentation and innovation will be exploited to advance CINCs' [Commander in Chief] C2 capability.

Although the JC2ASG report out is still being finalized, efforts are already underway under a Memorandum of Agreement [MOA] signed by the three Commanders and me in October 1998 to establish the Joint C2I2 Group [JC2I2G]. Under the JC2I2G MOA, three CINC Integration Program Offices [CIPO] and a Joint Forces Program Office [JFPO] have been stood up and are expected to be fully staffed toward the late summer or early fall 1999. The CIPOs are staffed with personnel from each of the three commands, while the initial JFPO is being co-hosted by the CIPO at SPAWAR. Cognizance for the CINCs has been divided up among the CIPOs, with the JFPO to maximize common C2I2 solutions. DISA has agreed to support the efforts of the JC2I2G. Discussions are also underway with USACOM [U.S. Atlantic Command] under its new mission as CINC Integrator, and hence will be the focus for the JFPO. Initial visits to each of the CINCs have been done, and an initial set of problems is being examined.

The JC2I2G is a complement or supplement of existing capabilities from my organization, DISA, Joint Staff, or other organizations chartered to assist the CINCs. The reporting and issue resolution processes are being established. As a minimum, the JC2I2G will have quarterly IPRs [In-Process Review] with Dr. Gansler and me. The first of the IPRs was recently held with the next expected in the July timeframe. The funding for the CIPOs is initially being taken out of existing budgets and will capitalize on existing support staffs collocated at various CINC facilities. The JC2I2G will make use of the existing interconnection of their test beds, and in the future to both the Joint Interoperability Test Command, and eventually to the Joint Battle Center located at USACOM.

"Before starting a COTS software acquisition, program managers should do sufficient market research to determine whether a COTS package is available that can meet documented system requirements without modification."

The CIPOs will also make use of the Architecture products (e.g,. CINC Architectures, JTA, DII COE) being developed with assistance from, or under the direction of, my organization's Information Integration and Interoperability Directorate. The I3 Directorate is also determining how the JC2I2G will fit into the reengineering of the DoD process for information interoperability.

Q

You earlier mentioned "GNIE." A steering group for this effort has now been formed. What's the relationship of GNIE on existing initiatives like the JTA and the COE?

A

The GNIE will use and/or incorporate any and all initiatives that deal with the information enterprise within the Department. Though this incorporation of initiatives can only be accomplished in stages given the vast scope of the DoD enterprise, certain initiatives will be incorporated in the initial stage of GNIE. The JTA and the COE are examples. The policies and strategies of GNIE will incorporate the JTA and its concepts of compliance with standards. The JTA also forms one of the three architecture views of the DoD information enterprise architecture and thus of the GNIE. The other two are the Joint Operational Architecture and the Joint Systems Architecture. The concept of the COE will be incorporated into the physical/systems architecture of the GNIE. Though this concept of the GNIE COE may be somewhat different than the current COE concept and strategy, the COE will be an important construct in the overall structure of the information enterprise.

Q

There is a short list of generic acquisition "best practices" in the current DoD 5000.2-R. Given the systemic problems DoD has encountered regarding acquisition of software-intensive systems, it seems a more specific listing of software acquisition best practices might indeed be warranted. What are your thoughts on this?

A

On May 1, 1997, the USD(A&T), the USD(Comptroller) and the DoD CIO